Ceyda Özdemir

Appendix to DuD 11/26

1 AI-generated Learning Modules and its Quality Assessment

To analyze the AI-generated learning modules on technical and organizational measures (TOMs) under Art. 32 GDPR and Section 5c EnWG, on 1 June 2026, OpenAI's ChatGPT, Anthropic's Claude and Microsoft's Copilot were asked to create learning modules for employees in the energy sector, based on an identical prompt, namely: *"Please create a text-based self-learning module for employees in the energy sector with a maximum length of 2,500 characters[1] including spaces. The self-learning module should explain that technical and organizational measures can serve different regulatory requirements and protection objectives and are often implemented jointly within an organization in the energy sector. Using Article 32 GDPR and Section 5c of the German Energy Industry Act (Energiewirtschaftsgesetz) as frameworks the module should explain which protected interests are at the core of each provision, where overlaps exist, and how technical and organizational measures interact in practice when they are required by different but concurrently applicable legal frameworks."*

Each following subsection of this appendix presents an AI-generated learning module followed by its corresponding assessments.

1.1 ChatGPT[2]

Learning Objective: Understand how technical and organizational measures (TOMs) can simultaneously fulfill different legal requirements and protection objectives in the energy sector.

Background: Organizations in the energy sector are often subject to multiple legal frameworks at the same time. Although these frameworks pursue different regulatory goals, they frequently require comparable technical and organizational measures. Therefore, a single measure may contribute to compliance with several legal obligations.

Example 1: Article 32 of the General Data Protection Regulation (GDPR) requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Protected interest: The primary objective is the protection of personal data and the rights and freedoms of natural per sons. Measures aim to ensure confidentiality, integrity, availability, and resilience of systems processing personal data.

Example 2: Section 5c EnWG requires energy-sector entities to take appropriate technical and organizational measures to ensure the security of network and information systems.

Protected interest: The focus is the secure and reliable operation of energy infrastructure and related network and information systems. The objective is to maintain the functionality, availability, and resilience of energy supply processes.

Where do the requirements overlap? Both provisions require risk-based technical and organizational measures. Typical examples include:

- Access and authorization management
- Authentication mechanisms
- Network segmentation
- Backup and recovery procedures
- Incident management processes
- Employee awareness and training

These measures can simultaneously support data protection and energy-sector cybersecurity objectives.

How do the measures interact in practice? A company may implement multi-factor authentication to protect personal data processed in IT systems (GDPR) while also reducing the risk of unauthorized access to systems relevant for energy operations (EnWG). Similarly, backup and recovery procedures can help restore personal-data processing activities and support the continuity of critical energy-sector services.

Key Takeaway: Technical and organizational measures should not be viewed in isolation. In the energy sector, the same measure often contributes to multiple legal requirements. Effective compliance therefore requires an integrated approach that considers both the protection of personal data and the security and resilience of energy-sector operations.

Assessment

Cross-application of Technical and Organizational Measures: The explanation provides accurate and sufficient information regarding the implementation of TOMs in the energy sector. However, the learning objective should have been given more precisely by giving reference to Art. 32 GDPR and Section 5c EnWG.

Protected Interest in Art.32 GDPR: The information is accurate and is consistent with the wording of Art. 32 GDPR. Additionally, further information regarding the responsible stakeholder is provided here.

Protected Interest in Section 5c of EnWG: The explanation provides accurate information regarding the protected interest but incomplete information regarding the responsible stakeholder. Section 5c (1) EnWG describes the responsible stakeholders as operators of energy supply networks, energy installations and digital energy services. Therefore, the term "energy sector entities" is oversimplified and incomplete.

[1] A limitation of lengths holds the advantage of an easier and fairer comparison between the different AI-Tools used. At the same time, the strict length limit is a limitation of this study, because AI-Tools might not be able to give all information or examples needed for understanding.

[2] Except for the assessment, this subchapter consists solely of text generated by OpenAI´s ChatGPT.

Overlaps between Provisions: The explanation provides only the risk-based approach as an overlapping requirement between both provisions. The response should also have included further important examples, such as documentation obligations and regular reviews. However, the list of overlapping TOMs which are suitable for implementation under both provisions is presented accurately.

Interplay of TOMs in Practice: The explanation provides accurate and sufficient illustrative examples of TOMs and how they can complement both provisions' purposes simultaneously.

1.2 Claude[3]

Why Do Two Laws Require the Same Measures? Energy sector organisations operate under several legal frameworks at once. Two that frequently overlap are Article 32 GDPR and Section 5c EnWG (German Energy Industry Act). Both mandate technical and organisational measures (TOMs) – yet serve distinct protection objectives.

Protected Interests at a Glance: Article 32 GDPR protects personal data. It requires measures ensuring confidentiality, integrity, availability, and resilience of processing systems. The core interest is the fundamental right to data protection.
Section 5c EnWG protects energy supply security. It obliges network operators and suppliers to implement IT security measures against cyberattacks that could disrupt supply. The core interest is public infrastructure security.

Where Overlaps Exist: Smart meters, SCADA systems, and customer portals process personal data and form part of critical infrastructure. A cyberattack on a metering system can simultaneously breach data protection law and endanger supply — triggering both provisions at once.
The same TOM — network segmentation, access controls, or encryption — can therefore satisfy Art. 32 GDPR and Section 5c EnWG simultaneously.

How TOMs Interact in Practice: Because both frameworks apply concurrently, organisations should adopt an integrated approach:

- Joint risk assessment: Analyse data protection and IT security risks together. Many threats — ransomware, insider access — are relevant to both.
- Shared measure catalogue: Document TOMs once and map each to its legal basis. This avoids duplication and aids audit readiness.
- Coordinated governance: Involve both the Data Protection Officer and IT Security Officer when designing measures.
- Unified incident response: An incident may trigger GDPR notification duties and reporting obligations under Section 11 EnWG. Processes must address both.

Key Takeaway: Different frameworks pursue different objectives — but their technical implementation often converges. TOMs work best when designed holistically: one documented set of measures satisfying multiple legal requirements, not isolated silos.

Assessment

Cross-application of Technical and Organizational Measures: The explanation is adequate to show the multi-level framework of TOMs, using the example of Art. 32 GDPR and Section 5c EnWG.

Protected Interest in Art. 32 GDPR: The information constitutes a weak response compared to the corresponding response from ChatGPT. Within the AI-generated text, the core interest under Art. 32 of the GDPR is oversimplified as the "fundamental right to data protection"; whereas in reality the core interest under Art. 32 GDPR is ensuring the security of personal data processing with the aim of protecting the personal data and the fundamental rights and freedoms of natural persons.

Protected Interest in Section 5c of EnWG: The explanation contains incomplete and inaccurate information. Although the scope of the EnWG is not limited solely to public infrastructure[4] and it protects network and information systems with the aim of ensuring an uninterrupted energy supply, the module oversimplifies that the core interest is the security of public infrastructure. Furthermore, the learning module refers to "network operators and suppliers" as the responsible stakeholders. This terminology neither accurately identifies the relevant stakeholders nor reflects the legal framework. The term "network suppliers" is vague and does not correspond to the legal framework. Furthermore, suppliers are not required to implement TOMs under Section 5c EnWG. Likewise, instead of the term "network operator," the legally accurate term "energy supply network operator" should have been used.

Overlaps between Provisions: The explanation provides overlapping TOMs between Art. 32 GDPR and Section 5c EnWG. However, it does not provide overlapping obligations between provisions such as risk assessment, documentation or regular review. On the other hand, the learning module identifies the conditions that enable parallel applicability between Art. 32 GDPR and Section 5c EnWG. In this respect, compared to the response from ChatGPT, Claude provides useful additional explanations on what is causing parallel applicability between two regulations. However, when considered as a whole, the explanation remains incomplete.

Interaction of TOMs in Practice: The explanation is sufficient and accurate as it provides various aspects for integrated implementation for TOMs along with additional information on how these different aspects can benefit organizations.

1.3 Copilot[5]

Technical and organizational measures (TOMs) often serve multiple regulatory purposes at once. In the energy sector,

[3] Except for the assessment, this subchapter consists solely of text generated by Anthropic´s Claude.

[4] Bourwieg/Hellermann/Hermes/Hellermann, EnWG § 109, Mn. 11

[5] Except for the assessment, this subchapter consists solely of text generated by Microsoft´s Copilot.

this is especially visible when comparing Article 32 GDPR and Section 5c EnWG. Both require robust safeguards, but they protect different core interests.

Core Protection Objectives:

- Article 32 GDPR — Protects personal data. Its focus is on confidentiality, integrity, availability, and resilience of systems processing personal information. The protected interest is the fundamental right to data protection.
- Section 5c EnWG — Protects the security of energy supply. It requires operators of energy installations and networks to implement an information security management system (ISMS) aligned with recognized standards. The protected interest is the continuous, reliable functioning of critical energy infrastructure.

Where the Requirements Overlap: Both frameworks demand

- Risk-based security
- Appropriate TOMs
- Continuous improvement
- Documentation and accountability

This overlap means that a single measure—such as access control, network segmentation, or incident response procedures—can satisfy obligations under both legal regimes.

How TOMs Interact in Practice: In energy organizations, TOMs are rarely implemented in isolation. Instead, they form integrated controls that map to multiple requirements:

- A central identity and access management system protects personal data (GDPR) and prevents unauthorized access to operational technology (EnWG).
- A business continuity plan ensures availability of personal data (GDPR) and supports uninterrupted energy supply (EnWG).
- A security incident response process fulfills GDPR breach response duties while also meeting EnWG expectations for handling security events affecting energy systems.
- Because the risk environments overlap—IT/OT convergence, cyber physical threats, and regulatory scrutiny—organizations typically design TOMs within a unified governance framework such as an ISMS. This avoids duplication, reduces cost, and ensures consistent security across personal data processing and critical infrastructure operations.

Key Takeaway

Although GDPR and EnWG pursue different protected interests, their security expectations are compatible. By designing TOMs that address both data protection and energy system resilience, organizations create a coherent, efficient, and legally compliant security posture.

Assessment

Cross-application of Technical and Organizational Measures: The explanation is accurate and sufficient to demonstrate that TOMs are regulated by various legal frameworks by using examples of Art. 32 GDPR and Section 5c EnWG.

Protected Interest in Art. 32 GDPR: The explanation is very similar to Claude's response in regard to oversimplifying the core interest of Art. 32 GDPR – the core interest of Art. 32 GDPR should have been explained as ensuring the security of personal data processing with the aim of protecting the personal data and the fundamental rights and freedoms of natural persons.

Protected Interest in Section 5c of EnWG: The explanation is unclear and incomplete in many aspects. Like other AI-generated learning materials, stakeholders which should implement TOMs under Section 5c EnWG are not fully listed, e.g. operators of digital energy services should have also been mentioned. Moreover, while the explanation regarding the core protected objective is not incorrect, it could have been more concise by explaining the protected interest as ensuring the security of network and information systems to maintain an uninterrupted energy supply. Additionally, the claim that Section 5c EnWG requires an ISMS aligned with recognized standards is imprecise: the provision requires a catalogue of individual measures ("IT-Sicherheitskatalog") rather than explicitly mandating the implementation of an ISMS. Although the security catalog pursuant to Section 5c EnWG has not yet been published, the previous version of the security catalogue already incorporates ISMS process elements, such as risk-analysis concepts and the evaluation of risk-management measures' effectiveness.[6]

Overlaps between Provisions: The explanation consists of accurate and sufficient information regarding the overlapping requirements between provisions along with the relevant examples of overlapping TOMs that complement both provisions' protected interests.

Interaction of TOMs in Practice: The explanation provides the most detailed answer compared to the other AI-generated learning materials. It presents accurate examples and explains how each measure complements the objectives of the respective provision. Furthermore, it explains why and to what extent an integrated approach to TOMs can be beneficial for energy organizations.

[6] Bundesnetzagentur, Festlegung-Erstellung eines IT- Sicherheitskatalogs nach § 5c Abs. 1-3 EnWG.